ANALYSIS OF INTRUSION DETECTION SYSTEM (IDS) IN BORDER GATEWAY PROTOCOL

By Muhammad Mujtaba

Principal Supervisor: Dr.Priyadarsi Nanda

Co- Supervisor: Prof. Xiangjian He

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY
UNIVERSITY OF TECHNOLOGY, SYDNEY
2012.

“Elevate yourself so high that even God, before issuing every decree of destiny, should ask you: Tell me, what is your intent?” – Dr. Allama Iqbal

Dedicated to

my mom, Mrs.Saira

CERTIFICATE OF AUTHORSHIP/ORIGINALITY

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of Candidate

_____

ACKNOWLEDGMENTS

It is a pleasure to thank the many people who made this thesis possible.

It is difficult to overstate my gratitude to my Ph.D. supervisor, Dr. Priyadarsi Nanda. With his enthusiasm, his vast experience and knowledge, and his great efforts to explain things clearly and simply, he helped reduce the complexity of this thesis and made it simple for me. Throughout my thesis-writing period, he provided encouragement, sound advice, good teaching, good company, and lots of good ideas.

I would like to thank Professor Xiangjian He for all the help and support he provided me in the areas of pattern recognition and network security; I would like to extend my sincere thanks to all my research fellow students for their contribution, feedback and for arranging weekly meetings for the exchange of cutting edge ideas which in all helped me with this research.

I wish to thank my good friends (Esha Dutt) - for proof reading and paper editing, Hamid Ghous (PhD candidate) for helping me with writing the computer program, getting through the difficult times and for all the emotional support, entertainment, and caring they provided.

I wish to thank my entire family for providing me with emotional and loving support. Lastly, and most importantly, I wish to thank my mum, Mrs. Saira, who raised me, supported me, taught me, and loved me. To whom I dedicate this thesis.

ABSTRACT

Border Gateway Protocol (BGP) is the de-facto inter-domain routing protocol used across thousands of Autonomous Systems (AS) joined together in the Internet. The main purpose of BGP is to keep routing information up-to-date across the Autonomous System (AS) and provide a loop free path to the destination. Internet connectivity plays a vital role in organizations such as in businesses, universities and government organisations for exchanging information. This type of information is exchanged over the Internet in the form of packets, which contain the source and destination addresses. Because the Internet is a dynamic and sensitive system which changes continuously, it is therefore necessary to protect the system from intruders. Security has been a major issue for BGP. Nevertheless, BGP suffers from serious threats even today, DoS attack is the major security threat to the Internet today, among which, is the TCP SYN flooding, the most common type of attack. The aim of this DoS attack is to consume large amounts of bandwidth. Any system connected to the Internet and using TCP services are prone to such attacks. It is important to detect such malicious activities in a network, which could otherwise cause problems for the availability of services.

This thesis proposes and implements two new security methods for the protection of BGP data plane, "*Analysis of BGP Security Vulnerabilities*" and "*Border Gateway Protocol Anomaly Detection using Failure Quality Control Method*" to detect the malicious packets and the anomaly packets in the network.

The aim of this work is to combine the algorithms with the Network Data Mining (NDM) method to detect the malicious packets in the BGP network. Furthermore, these patterns can be used in the database as a signature to capture the incidents in the future.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ACL	Access Control List
AH	Authentication Header
AR	Alarm Rate
AS	Autonomous System
ASN	Autonomous System Number
BCP	Best Common Practices
BGP	Border Gateway Protocol
CPU	Central Processing Unit
CSI	Computer Security Institute
CUSUM	Cumulative Sum
DDoS	Distributed Denial of Service
DoS	Denial of Service
DR	Detection Rate
EBGP	Exterior BGP
ESP	Encapsulating Security Payload
EWMA	Exponentially Weight Moving Average
FCE	Flow Connection Entropy
FP	False Positive
FQC	Failure Quality Control
FTP	File Transfer Protocol
GTSM	Generalized TTL Security Mechanism
HIDS	Host Intrusion Detection Sensor

HHH Hierarchical Heavy Hitter

HTTP Hyper Text Transfer Protocol

HTTPS Hyper Text Transfer Protocol Secure

IANA Internet Assigned Number Authority

IBGP Interior BGP

IDS Intrusion Detection System

IDSC Intrusion Detection Systems Consortium

IPS Intrusion Prevention System

IPSec Internet Protocol Security

IRR Internet Routing Registers

IRV Internet Routing Validation

ISP Internet Service Provider

KDD Knowledge Discovery and Data

LCL Lower Control Limit

MAC Message Authentication Code

MD Message Digestion

MED Multi-Exit Discriminator

MTU Maximum Transmission Unit

NADA Network Anomaly Detection Algorithm

NDM Network Data Mining

NIDS Network Intrusion Detection Sensor

NTM Network Traffic Management

OS Operating System

PCA Principal Component Analysis

PTA Pakistan Telecommunication Authority

PGBGP Pretty Good BGP

QoS Quality of Service

RIR Regional Internet Registries

ROC Receiver Operator Curve

RST Rough Set Theory

S-BGP Secured-BGP

SDM Security Device Manager

SHA Standard Hashing Algorithm

SIM Source IP Monitoring

SLA Service Level Agreement

SoBGP Secure Origin BGP

SPAN Switched Port Analyser

SVM Support Vector Machine

TCP Transport Communication Protocol

ToS Term of Service

TP True Positive

TTL Time to Live

UCL Upper Control Limit

UDP User Datagram Protocol

UPS Uninterruptible Power Supply

URCA Unsupervised Root Cause Analysis

VPN Virtual Private Network

WGLR Wavelet Generalized Likelihood Ratio